NAT Behavioral Requirements for Unicast TCP

Saikat Guha, Paul Francis

draft-hoffman-behave-tcp-03

IETF 64

Overview

- Based on definitions and assumptions in the UDP draft
- Started by Paul Hoffman; being moved forwards by Saikat Guha, Paul Francis
- Three basic goals/requirements:
    1. Allow TCP simultaneous open
    2. Specify response to unsolicited SYN
    3. Minimum timer values and mapping expiry

Background

- Recent paper [Guha, IMC 2005] : “Characterization and Measurement of TCP Traversal through NATs and Firewalls”
  - $>$ 120 NATs ($>$ 16 brands)
  - 8 approaches (2 real contenders)
- TCP NAT Traversal already works 85–90% of the time.
- Requirements based on problems we encountered

Requirement 1

- Allow all valid TCP packet sequences on an open mapping
  - Support TCP Simultaneous Open
  - Allow incoming connections that satisfy endpoint filtering requirements of NAT
  - Support Simultaneous Close
- Security considerations
  - Allows for existing strict NATs
  - Allows NATs that are just NATs (and not firewalls) to forward all TCP packets and be compliant

Requirement 2

- What is the response to an unsolicited SYN?
  - MUST NOT send a RST
  - may drop silently
  - may send ICMP soft-error
- Security considerations
  - ICMP soft-error prevents identity theft
  - but confirms presence of NAT

Requirement 3

- Mapping timers SHOULD be at least those from RFC 1122:
  - 4 minutes before first ACK in both direction (i.e. 4 min for 3-way SYN-SYNACK-ACK or simultaneous SYN/SYN-SYNACK/SYNACK)
  - 2 hours after the first ACKs and before FINs in both direction
  - 4 minutes after FINs in both directions
  - left unspecified for CLOSED state (think RST)
- Security considerations
  - leaves room for NAT to avoid DoS through NAT-generated keepalives

Requirement 3

- Timer values are SHOULD because RFC 1122 has them as SHOULD
- SHOULD send RST to both parties if mapping expires due to timeout
- Tracking TCP state requires NAT to track TCP sequence numbers and TCP Timestamp.
  - RECOMMENDED not REQUIRED

Summary

- Requirements:
  1. MUST Allow valid TCP packet sequences
     - TCP Simultaneous open etc.
  2. MUST not sent RST for unsolicited SYN
  3. SHOULD use RFC 1122 timers
- Security considerations updated

Questions?